Legislative Audit Division

State of Montana

Report to the Legislature

June 2006

Information System Audit

Montana State University – Electronic Research Data Security

Montana State University

This report addresses controls over the university's electronic research data storage infrastructure. It contains one recommendation to formally designate responsibility for research data security and implement and enforce a policy to define research data security requirements.

Direct comments/inquiries to:
Legislative Audit Division
Room 160, State Capitol
PO Box 201705
Helena MT 59620-1705

06DP-01

Help eliminate fraud, waste, and abuse in state government. Call the Fraud Hotline at 1-800-222-4446 statewide or 444-4446 in Helena.

INFORMATION SYSTEM AUDITS

Information System (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States Government Accountability Office.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting and computer science.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator Joe Balyeat, Vice Chair	Representative Dee Brown
Senator John Brueggeman	Representative Hal Jacobson
Senator Jim Elliott	Representative Christine Kaufmann
Senator Dan Harrington	Representative Scott Mendenhall
Senator Lynda Moss	Representative John Musgrove, Chair
Senator Corey Stapleton	Representative Janna Taylor

LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
Tori Hunthausen,
Chief Deputy Legislative Auditor

Deputy Legislative Auditors:
James Gillett
Jim Pellegrini

June 2006

The Legislative Audit Committee
of the Montana State Legislature:

A study conducted by the Carnegie Foundation for Advancement of Teaching ranked Montana State University-Bozeman in the top two percent of the country's institutions in terms of research. During fiscal year 2005, the university administered grant and contract sponsored research totaling $98 million. Montana State University-Bozeman anticipates sponsored research will exceed $100 million this year. We conducted an audit of the electronic research data security environment implemented at Montana State University. This report contains one recommendation to formally designate responsibility for research data security and implement and enforce a policy to define research data security requirements.

We wish to express our appreciation to the staff of Montana State University for their cooperation and assistance.

Respectfully submitted,

/s/ Scott A. Seacat

Scott A. Seacat
Legislative Auditor

Room 160, State Capitol Building, PO Box 201705, Helena, MT 59620-1705
Phone (406) 444-3122 FAX (406) 444-9784 E-Mail lad@mt.gov

Legislative Audit Division

Information System Audit

Montana State University – Electronic Research Data Security

Montana State University

Members of the audit staff involved in this audit were Jessie Solem and Nathan Tobin.

Table of Contents

Appointed and Administrative Officials

Montana State University – Bozeman	Geoffrey Gamble, President Montana State University-Bozeman
	Thomas McCoy, Vice President Office of Research, Creativity & Technology Transfer
	Jim Rimpau, Chief Information Officer Information Technology Center
	Virginia Key, Director Internal Audit

Executive Summary

Montana State University (MSU) is a research-intensive land grant university. The university encompasses four campuses located in Bozeman, Billings, Great Falls, and Havre.

In a March 3, 2006 article in *The Chronicle of Higher Education,* MSU-Bozeman was designated as a university with "very high research activity" based on a study conducted by the Carnegie Foundation for Advancement of Teaching. This designation is the highest distinction granted by the Carnegie Foundation and places MSU-Bozeman in the top two percent of the country's institutions in terms of research. During fiscal year 2005, the MSU-Bozeman Research, Creativity and Technology Transfer office administered grant and contract sponsored research totaling $98 million. The Billings campus also performs research activity, although not to the same degree as the Bozeman campus. The Billings campus currently is administering $600,000 in grant and contract funds used for sponsored research. MSU-Northern and MSU College of Technology-Great Falls campuses receive grant and contract monies; however, these campuses do not perform research.

Grant and contract funds support research activities resulting in the collection of data. The processes used to create research data are unique and the data created is often irreplaceable if lost or corrupted. Each campus is responsible for securing research data resulting from grant and contract sponsored activity. Universities are susceptible for computer intrusion attempts, because they have high-speed networks, vast amounts of storage, and a more open approach to sharing information because of their research mission. For this reason, it is important to provide security measures to protect the integrity and the intellectual and monetary value of research data, as well as the university's reputation as a research school. The scope of this audit is limited to the security of electronic research data at MSU-Bozeman and MSU-Billings.

We evaluated the electronic research data control environment using Board of Regents policy, university policy and procedures, data security practices implemented at similar universities, and generally

applicable and accepted information technology standards established by the IT Governance Institute. Audit work was conducted on both the Bozeman and Billings campuses.

On the Billings campus, approximately $600,000 in grant and contract funds are used by nine Principal Investigators (research project managers) to conduct sponsored research. During the course of our audit, we identified issues regarding physical access, user access control procedures, existence of a built-in account, and user workstation update practices. We believe these issues warrant management attention; however, these issues are not included in the report, but were discussed with MSU-Billings management. Upon our notification of these issues, MSU-Billings immediately addressed our concerns.

Principal Investigators on the MSU-Bozeman campus represented they applied some level of protection to secure research data. However, Principal Investigators have not been provided guidance to define the required level of data security. Research activity on the MSU-Bozeman campus has earned the university recognition as a top ranking research institution and research activity on the campus is expected to exceed $100 million this year. Given the importance of research to MSU-Bozeman, more emphasis could be placed on the security of electronic research data.

Chapter I – Introduction and Background

Introduction and Background

Montana State University (MSU) is a research-intensive land grant university. The university encompasses four campuses located in Bozeman, Billings, Great Falls and Havre, as well as the Montana Agricultural Experiment Station, Montana Extension Service and the Fire Services Training School.

In a March 3, 2006, article in *The Chronicle of Higher Education*, MSU-Bozeman was designated as a university with "very high research activity" based on a study conducted by the Carnegie Foundation for Advancement of Teaching. This designation is the highest distinction granted by the Carnegie Foundation and places MSU-Bozeman in the top two percent of the country's institutions in terms of research. During fiscal year 2005, the MSU-Bozeman Research, Creativity and Technology Transfer Office administered grant and contract sponsored research totaling $98 million. The Billings campus also performs sponsored research activity, although not to the same degree as the Bozeman campus. The Billings campus currently is administering approximately $600,000 in grant and contract funds used for research. MSU-Northern and MSU College of Technology-Great Falls campuses receive grant and contract monies; however, these campuses do not perform research.

Each campus is responsible for securing research data resulting from grant and contract sponsored activities. Research data is data compiled through grant or contract sponsored research for the academic pursuit of scholarly, economic, and technological advancement. The processes used to create research data are unique and result in data that is often irreplaceable. Security of this data is important to ensure research results are protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise.

Audit Objective

Universities are susceptible to computer intrusion attempts because they have high-speed networks, vast amounts of storage, and a more open approach to sharing information because of their research mission. For this reason, it is important to provide security measures

to protect the integrity and the intellectual and monetary value of research data, as well as the university's reputation as a research school. We conducted an audit to determine whether controls are in place to protect electronic research data from loss or unauthorized use or modification.

Audit Scope and Methodology

The audit was conducted in accordance with Government Auditing Standards published by the United States Government Accountability Office (GAO). We evaluated the control environment using Board of Regents policy, university policy and procedures, data security practices implemented at similar universities, and generally applicable and accepted information technology standards established by the IT Governance Institute.

The Board of Regents, the governing body for the Montana University System, implemented a policy in 2001 tasking each campus of the Montana University System to establish and maintain policies for the security of data. The scope of this audit is limited to the security of electronic research data at MSU-Bozeman and MSU-Billings. MSU-Northern and MSU College of Technology-Great Falls campuses receive grant and contract monies; however, these campuses do not perform research. Grant and contract monies received are used for such items as student retention, promotion of computer technologies in rural communities, and staff salaries.

On the MSU-Billings campus, approximately $600,000 is used by nine Principal Investigators (research project manager) to conduct sponsored research. On the MSU-Bozeman campus, 58 departments administered research and/or sponsored programs totaling $98 million; departments with the most expenditures include Veterinary Molecular Biology, Physics, Land Resources and Environmental Sciences, Cell Biology and Neurosciences, and Chemistry and Biochemistry.

MSU-Bozeman

The MSU-Bozeman campus uses a decentralized approach to research data security. Each Principal Investigator (PI) manages the

security of their electronically stored data. Research data is stored at various locations including individual workstations, removable media, department, subcontractor or centrally managed servers, and/or external computer hard drives. To gain an understanding of the electronic data security measures in place at MSU-Bozeman, we conducted a survey of PIs. The results of the survey were reviewed and security measures implemented by PIs were compared to data security measures established in other university environments similar to the Bozeman campus (i.e., student population and research ranking). We conducted interviews with MSU-Bozeman management and reviewed a report of thefts occurring on the MSU-Bozeman campus and a list of computer compromises reported by university personnel to determine: 1) the occurrence of campus-wide information technology hardware loss or theft and virus infections; and 2) to determine if PIs have reported information technology incidents. We analyzed the data gathered to determine the existence of vulnerabilities that threaten the security of electronic research data.

MSU-Billings

The MSU-Billings Information Technology Office is responsible for providing a data storage infrastructure. On the Billings campus, research data is stored on individual workstations and a centrally managed server. We evaluated the devices storing research data to determine whether controls are in place to protect electronic research data from loss or unauthorized use or modification. We reviewed computer configurations to ensure built-in user accounts were disabled and antivirus software was installed and current. We reviewed user access permissions and physical access controls to the server and workstations storing research data to determine if access was limited to authorized users. We interviewed MSU-Billings management and staff and used an automated audit tool to confirm only necessary software was installed on workstations, storage devices were up-to-date with security updates, and access control software existed. We reviewed data backup practices and schedules and identified controls for data recovery.

During the course of our audit, we identified concerns related to physical access, user access control procedures, existence of built-in accounts, and user workstation update practices. We believe these issues warrant management attention; however, these issues are not included in the report, but were discussed with MSU-Billings management. Upon our notification of these issues, MSU-Billings took steps to address our concerns.

Conclusion

Overall, the MSU-Billings Information Technology Office has implemented controls to provide a secure infrastructure for the storage of electronic research data. PIs on the MSU-Bozeman campus represented they applied some level of protection to secure research data. However, PIs have not been provided guidance to define the required level of data security. Research activity on the MSU-Bozeman campus has earned the university recognition as a top ranking research institution and research activity on the campus is expected to exceed $100 million this year. Given the importance of research to MSU-Bozeman, more emphasis could be placed on the security of electronic research data. The following chapter discusses vulnerabilities in MSU-Bozeman's research data storage infrastructure.

Chapter II – Bozeman Electronic Research Data Security

No Data Security Guidance

According to the MSU President, research data security is the responsibility of the Chief Information Officer (CIO) and the Vice President of the Office of Research, Creativity, and Technology Transfer. However, these individuals have not defined data security requirements and alternate individuals are managing electronic research data security. Currently, electronic research data security is managed by over 400 different PIs, who are the individuals responsible for the scientific and creative aspects of a grant and for the day-to-day management of a research project. Although PIs do not receive central guidance, they may receive data security guidance from other entities, such as the sponsoring organization or institutional review boards. We asked each PI to complete a survey regarding how they secure their research data. Of the 244 respondents, 168 represented they electronically store data. Seventy-nine percent of the PIs electronically storing data represented they receive no guidance or were unsure if guidance had been provided.

Research Data Vulnerabilities

To determine how effectively PIs are securing electronic research data, we reviewed the survey results to identify data security measures PIs represented they applied. We compared the security measures to controls implemented in other university environments similar in student population and research activity as MSU-Bozeman. Standard data security practices implemented in similar university environments include:

- Physical security measures to control physical access to the facility storing research data;
- Password security measures to safeguard against unauthorized electronic access to data;
- Data encryption to prevent unauthorized exposure of sensitive data;
- Antivirus software and update procedures to protect against installation of malicious software;
- Vendor security patch update procedures to correct security vulnerabilities and prevent computer compromise(s); and

- Data backup procedures to ensure continuity of research in the event of data loss or corruption.

We reviewed the survey results and, although most PIs indicated they applied some level of security, vulnerabilities exist that could result in data exploitation. These vulnerabilities are discussed below.

- *Physical Security*: Seventy-three of 168 PIs represented they are not physically securing the devices storing their research data. Forty-five of these PIs store their data on portable devices such as their personal computer's hard drive or removable media (i.e., CDs, flash drive). Use of portable devices increases the risk that theft or data loss will occur because the storage media is easily transported. Campus-wide, MSU-Bozeman reports approximately five thefts of information technology resources a year. Consequently, the potential exists that a device storing research data could be stolen.
- *Password Security*: Nineteen of 168 PIs represented they do not apply password authentication controls to control access to their data. The absence of password authentication controls allows electronic access to stored data to anyone with physical access to the storage device. This increases the risk for unauthorized data modification or loss. Implementation of physical security controls or data encryption can prevent unauthorized access and use of stored data. However, 8 of the 19 PIs represented they do not apply physical security or data encryption controls.
- *Data Encryption*: Data encryption converts data into a format that is unintelligible, preventing anyone except the intended recipient from reading that data. Encryption protects the confidentiality of sensitive information when physical security cannot be provided. Thirty-three of 168 PIs represented their data is confidential. Twelve of the 33 PIs represented they do not apply physical security or data encryption controls.
- *Antivirus Software*: Twenty-three of 168 PIs represented they have not implemented current virus protection measures. Antivirus software protects storage devices from malicious programs (i.e., viruses, worms) that can result in loss of computer system operability or data. Since 2002, there have been over 300 instances of reported virus infections on the MSU-Bozeman campus. Forty-four of these incidents were reported by active PIs.
- *Security Updates*: PIs electronically store research data on hardware devices. Hardware devices are delivered with software packages that make the device functional. Software systems are

complex, and it is common for security-related problems to be discovered only after the software is in widespread use. Identified software vulnerabilities create opportunities for unauthorized intrusions. To prevent security flaws from resulting in exploits, software vendors release security updates to fix identified software problems. Installing applicable vendor security updates reduces vulnerabilities to attack. Thirty-seven of 168 PIs represented they do not keep their storage devices up-to-date with the most recent vendor-released security updates. Consequently, vulnerabilities for malicious attacks and data loss, damage, or modification are created.

- *Data Backup*: Data backup practices allow the availability and integrity of information resources to be restored following security breaches or system failures. Data loss can result for many reasons, including lost or stolen data storage devices, unauthorized data modification or deletion, or data corruption. Thirty-eight of 168 PIs represented they do not perform data backups. Security weaknesses exist that could result in unrecoverable data loss for these PIs. Of the 38 PIs:
  - Twenty-three (60 percent) do not physically secure devices electronically storing their research data;
  - Nine (24 percent) do not implement password protection;
  - Seven (18 percent) do not apply antivirus software protection;
  - Sixteen (42 percent) do not apply current vendor security updates to storage devices.

The above areas are security weaknesses that could result in data compromise. Research data is unique and if lost or corrupted it is often irreplaceable because the processes used to compile data results are often dependent on the circumstances present when the data was initially created (i.e., test subjects used). In addition, accumulated research data is used to create new products and processes and if research data was compromised, the PI and the university not only risks loss of irreplaceable data but also future innovations.

Summary

PIs typically are not information technology professionals who are involved on a day-to-day basis with data security. Even though PIs are not information technology professionals, they are managing research data security and have not received guidance from

university management who are responsible for the security of research data.

Data Security Policies Outdated and Not Comprehensive

In 1992, a policy was developed to establish a system of classifying data with respect to the need for security and to institute guidelines for maintaining the security of each data classification. However, this policy is part of the university's outdated computing policy manual and has not been implemented or enforced by the university. Without an updated policy, guidelines have not been defined regarding how data should be secured.

A 2001 legislative audit report (01DP-05) identified the outdated computing policy manual as an issue and recommended the university update the manual to ensure an adequate level of security for its data and information technology resources. In the report, the university acknowledged the policies were outdated and indicated they would like to implement policies which encompass all four campuses of MSU because the computing environments are interrelated. As a result of the audit, the Board of Regents implemented a policy requiring each campus of the Montana University System establish and maintain policies for the security of data. However, the Board of Regents policy defined data as that which relates to the university's administrative system (i.e., financial, human resources, financial aid, or student records). Subsequently, the university has not addressed the security of research data.

Data Security Policy and Enforcement Responsibilities

Security of research data has not been implemented or enforced because the campus information technology department did not have clear responsibility over all campus functional areas. Until recently, the Chief Information Officer reported to the Vice President of Administration and Finance, who in turn reported to the President. This created the appearance that the information technology department (Information Technology Center) was supporting only the administrative aspect of university operation and no support was

provided to academic operations. As a result, the Information Technology Center (ITC) was unable to manage data security within the academic user community for enforcement purposes. In July 2005, MSU-Bozeman reorganized and the Vice President of Planning and Analysis also became the Chief Information Officer to illustrate ITC supports all campus operations.

As part of the reorganization, the university created a framework to bring the academic and administrative campus communities together for decision-making purposes. The Chief Information Officer is relying on the campus community to create, develop, and approve policy for data security. However, the Montana State University President stated that the Vice President of the Office for Research, Creativity and Technology Transfer and the Chief Information Officer are responsible for the security of electronic research data. On the Bozeman campus, there is not a clear assignment and designation of authority regarding who is responsible for the security of research data. PIs have assumed responsibility for managing research data security and guidance has not been provided to define data security requirements.

Recommendation #1

We recommend the university:

A. Formally designate responsibility for electronic research data security; and

B. Implement and enforce a policy to address electronic research data security requirements.

Agency Response

MONTANA
STATE UNIVERSITY

June 2, 2006

Legislative Audit Division
Room 160, State Capitol
P.O. Box 201705
Helena, MT 59620-1705

RE: Montana State University - Electronic Research Data Security Audit - 06DP-01

Dear Sirs:

Montana State University has recently undergone an audit of its electronic research data security as conducted by the Legislative Audit Division. As a result of this audit one recommendation was made and we would like to take this opportunity to respond to this recommendation.

Recommendation #1
We recommend the University:

A. Formally designate responsibility for electronic research data security; and

B. Implement and enforce a policy to address electronic research data security requirements.

MSU Response

Montana State University concurs with Recommendation #1 and will designate the Assistant Vice President for Research, currently Leslie Schmidt, as the person responsible for addressing this issue. She is a member of MSU's Data Security Committee and will immediately draft and implement a policy outlining specific data security requirements specific for the research community on campus. This will be distributed to all faculty as well as being included on the Vice President for Research website, the Principal Investigator's "How To" Manual and discussed at new faculty orientation conducted each fall. In

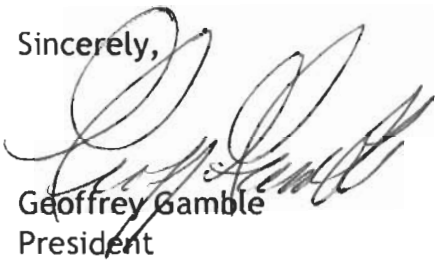
Office of the President
211 Montana Hall
P.O. Box 172420
Bozeman, MT 59717-2420
www.montana.edu

Tel (406) 994-2341
Fax (406) 994-1893

addition, the internal routing document, Proposal Clearance Form, will add a line that requires Principal Investigators to certify they have read and will adhere to the research data security policy.

Please do not hesitate to contact me should you have any questions,

Sincerely,



Geoffrey Gamble
President

GG/sm